時刻認証業務（リンキング方式）

[定義]

時刻認証におけるリンキング方式とは、時刻認証事業者（TSA）が複数のタイムスタンプ付与対象文書のハッシュ値を関連づけたリンク情報を生成してタイムスタンプトークンに含め、各タイムスタンプトークンを他の多数のタイムスタンプトークンに依存させることによってその信頼性を確保する方式である。

リンキング方式の時刻認証サービスでTSAが発行するタイムスタンプトークンには、タイムスタンプ付与対象文書のハッシュ値、タイムスタンプ付与時刻、そしてタイムスタンプ発行時に生成されたリンク情報または、リンク情報を用いたタイムスタンプ検証に必要な情報が含まれる。

本認定基準においては、タイムスタンプトークン検証の信頼性をTSAが保持する照合用データの完全性によって確保する方式に限定する。したがって、TSAはリンク情報をはじめタイムスタンプの照合に必要な情報を完全な形で保管するとともに、一連のリンク情報の代表値の明証化により、照合用データ全体の完全性を担保しなければならない。このため、本方式では、照合用データの完全性を担保するために生成したリンク情報は、その生成のプロセスに関与した全てのタイムスタンプトークンの付与対象電子文書のハッシュ値の要約となるように生成される。

タイムスタンプの検証の際は、検証者（タイムスタンプトークン保有者）がタイムスタンプ付与対象文書のハッシュ値を計算し、得られたハッシュ値とタイムスタンプトークンに含まれるハッシュ値との一致を確認する（ハッシュ値確認）とともに、タイムスタンプトークンを含む照合要求情報をTSAへ送り、TSAは送られてきたタイムスタンプトークンに含まれるハッシュ値およびリンク情報と保管している照合用データとの整合性を確認（照合）し、照合結果情報を検証者へ通知する。

リンキング方式の時刻認証サービスでは、タイムスタンプの有効性は照合用データの完全性に依存している。TSAは照合用データをアルゴリズム的に検証可能なものとし、また十分な信頼性を有する運用により保護する。

関連する標準：ISO/IEC18014-3, ISO/IEC18014-1

関連用語の定義
リンク情報
TSAがタイムスタンプ付与対象文書のハッシュ値同士、タイムスタンプ付与対象文書のハッシュ値と他のリンク情報またはリンク情報同士の３種類の組合わせのいずれかを含む情報を、検証が可能でかつ一方向性・衝突困難性を有する方法で連結させた情報

照合用データ
TSAがタイムスタンプ照合のために、タイムスタンプトークン生成時に記録・保管するリンク情報を含む情報

完全性
情報および処理方法が、正確であることおよび完全であることを保護すること

検証
タイムスタンプトークン保有者が、タイムスタンプトークンが真正で有効であることを確認するための一連の行為を指す。リンキング方式の検証は次の２つのプロセスで構成される。
１．ハッシュ値確認：タイムスタンプ付与対象文書のハッシュ値を計算し、タイムスタンプトークンに含まれるハッシュ値との一致を確認するプロセス
２．照合：タイムスタンプトークン保有者がTSAへ送ったタイムスタンプトークンと、TSAが保管している照合用データとの整合性をTSAが確認するプロセス

明証化
明証化とは、TSAが管理する照合用データの完全性を担保するために生成したリンク情報の代表値を、あらかじめ定められた規則に従って公開する行為を指す。

照合要求情報
タイムスタンプトークン保有者（照合要求者）がタイムスタンプトークンの検証を行う際に、照合のためにTSAに送る情報。照合要求情報には、タイムスタンプトークンが含まれる。

照合結果情報
TSA照合の結果を照合要求者へ通知する際にTSAが照合要求者へ送る情報。照合結果情報には、照合対象のタイムスタンプトークンを特定するための情報と、照合結果が含まれる。

照合用データおよび明証化に求められる要件
・ 一連の照合用データは、照合するタイムスタンプトークンに含まれるリンク情報と、明証化されたリンク情報の代表値との整合性をアルゴリズム的に証明できるものであること
・ 発行したタイムスタンプトークンから該当する照合用データの範囲が一意に特定できるように記録すること
・ 照合用データの記録は、タイムスタンプトークンの生成時に、遅滞なく行われること
・ リンク情報の明証化は、タイムスタンプの発行量などをもとに適切な頻度で行うこと

TSA時計
タイムスタンプトークンに含まれる時刻を生成するタイムスタンプサーバの時計

時刻ソース
TSAが時刻源として参照している認定TAAの時計
運用規程
TSAが公開する時刻認証業務についての基本的内容（ポリシー）と運用に関する基本的事項を明記した文書。TPS又はTP/TPSと表現されている場合もある。

利用者
TSAに対してタイムスタンプトークン発行要求を出してタイムスタンプトークンを受け取る者。タイムスタンプトークンを用いたアプリケーションサービスを行う事業者は利用者である。

検証者
タイムスタンプトークンの有効性検証を実施しようとする者
以上

（１）　技術基準

項目	基準（遵守事項）	エビデンス例
１　タイムスタンプトークンの時刻	タイムスタンプトークンに含まれる時刻は、TSA時計により生成されること	運用規程 TSA時計に関した技術資料
２　精度	TSA時計は、認定TAAから時刻配信を受け、UTC (NICT)に対し±1秒以内で同期していること	運用規程 時刻監査記録
３　精度の証明	TSA時計の品質を証明する手段を持つこと	
１ 認定を受けたTAAからの時刻配信	第三者もしくは時刻認証業務とは権限分離された組織が運営し、時刻配信業務についてタイムビジネス信頼・安心認定を受けたTAAから時刻配信を受けていることを証明できること	運用規程 TAAとの契約書類 リポジトリ情報
２ 認定を受けたTAAによる時刻監査	第三者もしくは時刻認証業務とは権限分離された組織が運営し、時刻配信業務についてタイムビジネス信頼・安心認定を受けた機関がTAAとしてTSA時計の時刻監査を行っていることを証明できること	運用規程 時刻監査記録 TAAとの契約書類 タイムスタンプトークン（TACを含む場合） リポジトリ情報
４　タイムスタンプサービス等の特定	タイムスタンプサービス等を特定する手段および、なりすまし対策を講じること	
１ 時刻配信を受ける機器の特定（TAA-TSA間）	時刻配信を受けるTAAの配信元機器の特定および認証可能な手段を用いること	時刻配信時の特定方法を説明する資料 例：TAAとの契約時の申請フォーマット、TAAの時刻監査報告、トークンなど

<table>
<tr><td>２ タイムスタンプサービスの特定（利用者→TSA）</td><td>利用者からタイムスタンプトークンの発行要求を受け付ける際には、時刻認証サービスの特定が可能な手段を用いること</td><td>サービスを特定する方法についての資料
例：SSL認証等</td></tr>
<tr><td>５　安全な通信路</td><td>時刻認証業務に係る通信では、セキュリティ対策がなされていること</td><td></td></tr>
<tr><td>１ TAA-TSA間</td><td>TAA-TSA間の通信はセキュリティ対策（なりすまし、改ざん、暗号化の対策など）がなされていること</td><td>技術仕様書
利用契約書類</td></tr>
<tr><td>２ TSA-利用者間</td><td>利用者とTSA間の通信はセキュリティ対策（なりすまし、改ざん、暗号化の対策など）がなされていること</td><td>技術仕様書
利用契約書類
例：SSL通信等</td></tr>
<tr><td>３ 暗号技術</td><td>時刻認証業務の通信路の安全性を公開鍵暗号技術または共通鍵暗号技術により実現する場合、電子政府における調達のために参照すべき暗号リスト(CRYPTREC暗号リスト）（平成25年3月1日に総務省、経済産業省が公表したもの）において電子政府推奨暗号リストに記載された暗号技術を用いること。
ただし、2015年1月1日以前に認定された事業者においては、SHA-1については、SSL3.0、TLS1.0/1.1/1.2、VPN、およびTSAが利用者識別に用いるCMS署名ならびに時刻配信監査時の認証、改ざん検知に用いるHMACにおいて互換性維持のために利用することを当面可とする。また、128-bit RC4については、SSL(TLS1.0以上）での利用を当面認める。</td><td>運用規程
安全性レベルの証明資料</td></tr>
<tr><td>６　タイムスタンプトークンのTSAポリシーへのリンク</td><td>タイムスタンプトークンには、TSAポリシーの識別情報、リファレンス情報、ハッシュ値など、TSAポリシーを一意に特定できる情報を含めること</td><td>運用規程
タイムスタンプトークン</td></tr>
<tr><td>７　タイムスタンプトークンのデータ形式</td><td>タイムスタンプトークンのデータ形式を、明確に定義し、運用規程に記載・公開していること</td><td>運用規程
タイムスタンプトークン</td></tr>
<tr><td>８　タイムスタンプトークンに含むべき情報</td><td>以下の情報をタイムスタンプトークンに含めること（〇はタイムスタンプトークンに必須、△はタイムスタンプトークンまたはTSAポリシー・リポジトリに含める）
<table>
<tr><th>含むべき情報</th><th></th></tr>
<tr><td>TSAのポリシーリンク</td><td>〇</td></tr>
<tr><td>時刻情報</td><td>〇</td></tr>
<tr><td>タイムスタンプ対象データのハッシュ値</td><td>〇</td></tr>
<tr><td>使用するハッシュアルゴリズム(OID)</td><td>〇</td></tr>
<tr><td>時刻精度</td><td>△</td></tr>
<tr><td>時刻ソース</td><td>△</td></tr>
<tr><td>発行者情報</td><td>△</td></tr>
<tr><td>検証のための情報
・リンク情報の代表値の明証化方法
・検証先情報</td><td>
△
△</td></tr>
<tr><td>有効期限</td><td>△</td></tr>
<tr><td>リンク情報</td><td>〇</td></tr>
</table></td><td>運用規程
タイムスタンプトークン</td></tr>
<tr><td>９　タイムスタンプトークンに含むべきでない情報</td><td>タイムスタンプトークンにはタイムスタンプの要求者の情報は含めないこと</td><td>運用規程
タイムスタンプトークン</td></tr>
<tr><td>10　タイムスタンプトークンの時刻の品質</td><td>TSAは（１）２項で定められた時刻精度を満たしていないタイムスタンプトークンの発行を防止するための措置を講じること
当該措置としてタイムスタンプトークンに含まれる時刻を外部の参照時計を用いて監視する場合、異常発生時には異常が明示され、また時刻差が記録されること</td><td>運用規程
システム構成概略図
処理フロー
時刻監視の仕組みと記録されるログについての説明資料</td></tr>
</table>

11　電子文書のハッシュ値を得るためのハッシュ関数	タイムスタンプトークンの付与対象となる電子文書のハッシュ値を得るためのハッシュ関数は、電子政府における調達のために参照すべき暗号リスト(CRYPTREC暗号リスト）（平成25年3月1日に総務省、経済産業省が公表したもの）において電子政府推奨暗号リストに記載された暗号技術を用いること	運用規程 タイムスタンプトークン 安全性レベルの証明資料
12　リンク情報の生成に用いるハッシュアルゴリズム	リンク情報の生成が以下の条件を満たすアルゴリズムにより安全に行われ、照合用データの完全性を担保できること ・ リンク情報は、その生成のプロセスに関与した全てのタイムスタンプトークンの付与対象電子文書のハッシュ値の要約となるように生成されること ・ リンク情報は、検証が可能でかつ一方向性・衝突困難性を有する形の連結により生成される必要があるため、元となる情報を結合したデータに対して、以下の基準を満たす安全なハッシュ関数を適用して計算されること リンク情報を生成するためのハッシュ値を計算するアルゴリズムとして、電子政府における調達のために参照すべき暗号リスト(CRYPTREC暗号リスト）（平成25年3月1日に総務省、経済産業省が公表したもの）において電子政府推奨暗号リストに記載されたハッシュ関数で確認される安全性以上のハッシュ関数を使用してリンク情報を生成すること	運用規程 タイムスタンプトークン 安全性レベルの証明資料
13　タイムスタンプトークンの生成処理	正しい時刻情報を含むタイムスタンプトークンの生成処理において、以下の要件を満たすプログラム等を実装していること	
1 当該プログラム等の完全性/正確性	時刻情報の取得からタイムスタンプトークンの生成に至るまでのプログラム等が正確に動作することを証明できること	当該プログラム機能仕様書 ソースコード資料および実動作確認 事業者が行った当該プログラムの試験項目および試験結果の確認
2 当該プログラム等の改ざんへの対策	当該プログラム等の改ざんを防止または検知する仕組みを備え、検知した場合には検知の結果を記録すること	改竄検出ソフトウェアの利用やプログラム自身の定期的なタイムスタンプ取得・保管、ハードウェアレベルの保護等
3 生成処理の実行の確認	タイムスタンプトークンの生成に係る正常なプロセスが動作していること、および時刻認証業務に不要なプロセスが動作していないことを確認する仕組みを備え、不正な状態を検知した場合には検知の結果を記録すること	技術仕様書および実動作確認 (例：動作しているプロセス名の確認および正常なプロセス名リストとの比較結果の記録等)
4 当該プログラムを含むサーバのすり替えへの対策	正しい時刻情報ならびに完全なプログラムが、正当なサーバ内で確かに用いられていることを証明できること	・SSL認証と管理者による秘密鍵の管理 ・監視カメラによる監視および監視データ保管期間根拠等の説明資料
5 タイムスタンプトークンと照合用データ	照合用データは、生成したタイムスタンプトークンを一意に特定できること	照合用データの仕様 タイムスタンプトークン
14　照合用データの保管処理	生成した照合用データの保管処理において、以下の要件を満たすプログラム等を実装していること	
1 当該プログラム等の完全性/正確性	タイムスタンプトークンの生成から照合用データの保管に至るまでのプログラム等が正確に動作することを証明できること	当該プログラム機能仕様書およびソースコード資料および実動作確認 事業者が行った当該プログラムの試験項目および試験結果の確認
2 当該プログラム等の改ざんへの対策	当該プログラム等の改ざんを防止または検知する仕組みを備え、検知した場合には検知の結果を記録すること	改竄検出ソフトウェアの利用やプログラム自身の定期的なタイムスタンプ取得・保管、ハードウェアレベルの保護等
3 保管処理の実行の確認	照合用データの保管に係る正常なプロセスが動作していること、および時刻認証業務に不要なプロセスが動作していないことを確認する仕組みを備え、不正な状態を検知した場合には検知の結果を記録すること	技術仕様書および実動作確認 (例：動作しているプロセス名の確認および正常なプロセス名リストとの比較結果の記録等)
4 当該プログラムを含むサーバのすり替えへの対策	完全なプログラムが照合用データの保管において、正当なサーバ内で確かに用いられていることを証明できること	・SSL認証と管理者による秘密鍵の管理 ・監視カメラによる監視および監視データ保管期間根拠等の説明資料

15　照合用データの完全性	タイムスタンプトークンの照合用データを生成後安全に記録し、完全性を維持するため、以下の要件を満たしていること	
1 照合用データの保管	照合用データは生成後、遅滞なく冗長化されたストレージへ保管すること	技術仕様書 （例：RAID1やRAID5等の多重化）
2 照合用データの完全性	リンク情報の代表値を明証化することにより照合用データの完全性が証明できること。照合用データは、いったん記録された後は情報の書換え、順序変更、挿入、削除などの変更操作ができないか、または変更操作が行われた場合には確実に検知できる方式で記録されること	技術仕様書 【想定される対策例】 ・ハードウェア技術を含む防止・検知策（例：HSMや書換え不可能で順序性の担保されたHDDに保管する） ・ソフトウェア技術による防止策（すり替えに要する技術的複雑性、時間的・経済的コストを非現実的なレベルに引き上げることで事実上の防止策とみなす。例：リンク情報の生成）
16　タイムスタンプトークンの照合処理	タイムスタンプトークンの照合処理において、以下の要件を満たすプログラム等を実装していること	
1 当該プログラム等の完全性/正確性	タイムスタンプトークンの照合を行うプログラム等が正確に動作することを証明できること	当該プログラム機能仕様書およびソースコード資料および実動作確認 事業者が行った当該プログラムの試験項目および試験結果の確認
2 当該プログラム等の改ざんへの対策	当該プログラム等の改ざんの防止または検知の仕組みを備え、検知した場合には検知の結果を記録すること	改竄検出ソフトウェアの利用やプログラム自身の定期的なタイムスタンプトークン取得・保管 ハードウェアレベルの保護等
3 照合処理の実行の確認	タイムスタンプトークンの照合に係る正常なプロセスが動作していること、および時刻認証業務に不要なプロセスが動作していないことを確認する仕組みを備え、不正な状態を検知した場合には検知の結果を記録すること	技術仕様書および実動作確認 (例：動作しているプロセス名の確認および正常なプロセス名リストとの比較結果の記録等)
4 当該プログラムを含むサーバのすり替えへの対策	完全なプログラムがタイムスタンプトークンの照合において、正当なサーバ内で確かに用いられていることを証明できること	・SSL認証と管理者による秘密鍵の管理 ・監視カメラによる監視および監視データ保管期間根拠等の説明資料
17　安全な照合手段の提供	タイムスタンプトークン照合処理では、セキュリティ対策（なりすまし、改ざん、盗聴の対策、など）が行われた通信路上で検証者とTSA間の照合プロトコルを実行すること	IF仕様書
18　タイムスタンプトークン照合処理の要件	以下の要件を満たす適切なタイムスタンプトークン照合処理を提供すること	
1 タイムスタンプトークン照合要求データ	タイムスタンプトークン照合要求データのフォーマットが検証者に明確に提示されていること	運用規程
2 タイムスタンプトークン照合処理	TSAは、タイムスタンプトークン照合要求データ形式に不備がある場合、検証者へエラー情報を返却すること	エラー情報種別についての説明資料
	TSAは、タイムスタンプトークン照合データの妥当性を検査し、その照合結果データを検証者へ返却すること	検証手段の仕様書 説明資料 デモ
3 タイムスタンプトークン照合結果データ	タイムスタンプトークン照合結果データの中に、対応する照合要求データのタイムスタンプトークンもしくはタイムスタンプトークンの識別子を含むこと	運用規程
	タイムスタンプトークン照合結果データの中に、照合要求されたデータに対するタイムスタンプトークン照合の結果を含むこと	運用規程
	照合結果データから、検証者がタイムスタンプトークンのデータ形式の崩れや改ざんの有無を判別できること	照合結果データサンプル 判別のデモ
	タイムスタンプトークンおよび照合要求データが有効である場合、照合結果データから、検証者が元文書の改ざんの有無を判別できること	照合結果データサンプル 判別のデモ

19　タイムスタンプトークン照合用ツールの要件	利用者自身がタイムスタンプトークンを照合するためのタイムスタンプトークン照合用ツールをTSAが利用者に提供する場合（ISO/IEC 18014-3 [2nd edition 2009-12-15] で規定されている「Extended operation」に対応している場合は除く）、次の要件を満たす適切なツールを提供しなければならない。また、照合用ツールの提供に先立ち、認定機関に対して利用者が継続して検証をできるための方法を説明すること。	
1 照合プログラム等の完全性/正確性	タイムスタンプトークンの照合を行うプログラム等が正確に動作することを証明できること	下記の場合に則して指定されたエビデンスを提出すること A.　当該プログラムが自社開発である場合(以下の両方を提出すること) ・事業者が行った当該プログラムの試験項目および試験結果もしくは第３者によるプログラムの品質評価結果 ・ソースコード資料もしくはソースコードの改ざんを検知できるエビデンス(タイムスタンプ等) B.　当該プログラムが他ベンダーの製品の場合(以下の両方を提出すること) ・事業者が行った当該プログラムの試験項目および試験結果、もしくは第３者によるプログラムの品質評価結果 ・当該プログラムが認定制度の基準に合致していることを保障する製造ベンダーの宣言書、ただしそれを提出できない場合は、当該「タイムスタンプ照合処理」の基準各項に関する説明書類
2 照合プログラム等の改ざんへの対策	当該プログラム等の改ざんの防止または検知の仕組みを備えること	技術仕様書 【想定される対策例】 プログラムの暗号化、コードサイニング証明書、タイムスタンプ、ハッシュ値の公開、ハードウェアレベルの保護等
3 照合用データの完全性	ツールに含まれる照合用データの完全性が証明できること。照合用データは情報の書換え、順序変更、挿入、削除などの変更操作ができないか、または変更操作が行われた場合には確実に検知する仕組みを備えること。	技術仕様書および実動作確認 【想定される対策例】 照合用データの暗号化、タイムスタンプ、ハッシュ値・リンク情報など照合用データの完全性を保証するための情報の公開、ハードウェアレベルの保護等
4 タイムスタンプトークン照合処理の要件	技術基準第18項で要求される適切なタイムスタンプトークン照合処理を提供すること	運用規程 照合結果データサンプル 判別のデモ

（２）運用基準

項目	基準（遵守事項）	エビデンス例
1　提供する業務の明確化	時刻認証事業者が提供する業務を明確に定め、以下の事項を含んでいること	
1 タイムスタンプトークンの生成・発行	利用者のリクエストに応じてタイムスタンプトークンを生成・発行すること	運用規程 サービス約款
2 時刻認証業務で使用する全ての時計の時刻管理	時刻認証業務で使用する全ての時計の時刻を十分な精度に維持すること	運用規程 サービス約款
3 時刻認証業務で使用する鍵の生成と管理	時刻認証業務で暗号鍵を使用する場合は、それらの暗号鍵を安全に生成し、管理すること	運用規程 サービス約款
4 時刻認証業務で使用するハッシュ関数が危殆化した場合の措置	時刻認証業務で使用するハッシュ関数の危殆化が発覚した場合は、速やかに当該ハッシュ関数の使用を中止するとともに利用者に連絡すること	運用規程 サービス約款
5 リンク情報代表値の生成と明証化	あらかじめ定められた規則に従って、リンク情報代表値の生成と明証化を行うこと	運用規程 サービス約款
6 タイムスタンプトークン照合	利用者または検証者のリクエストに応じてタイムスタンプトークンの照合を行うこと	運用規程 サービス約款

7 時刻認証業務で使用するハッシュ関数の危殆化が予想される場合の措置	時刻認証事業者は、タイムスタンプトークン生成で用いるハッシュ関数の危殆化が予測される事態になった場合に実施すべき次の対応策を策定しておくこと (a) 当該タイムスタンプトークンの発行停止予定日の決定と関係者への周知・報告 (b) 必要に応じて新たなハッシュ関数を用いたサービスへ移行すること (c) 有効性を維持する方法の関係者への周知・報告	運用規程 サービス約款
2 責任範囲の明確化	時刻認証事業者自身の責任と保証の範囲に関するポリシーを開示すること	
1 賠償責任	時刻認証事業者が負う賠償責任について開示すること	運用規程 サービス約款
2 免責事項	時刻認証事業者の免責事項について開示すること	運用規程 サービス約款
3 組織・人事管理	適切な組織構成および開発・運用維持、信頼性確保、可用性確保に対処できる能力・体制を確保すること	
1 組織構成	独立性が確保された組織が時刻認証業務を担当すること	組織図
2 専門性	時刻やセキュリティに関する専門性の優れた要員を配置すること また、適切な業務運営が行われるための教育訓練を行うこと	担当部署の組織図 各役職の役割・要件の規定 教育訓練の記録または計画書
3 内部牽制機能	事故を未然に防ぐために、部署内での内部牽制が働く構造、業務手順になっていること	時刻配信に関する業務手順書 承認フロー（関係部分のみ）
4 業務監査	部署外からの業務監査等のチェック機能が働くこと	監査主体と事業担当部署の責任上独立が確認できる組織図
5 事故発生時処理	事故発生時に、その発生源が特定できること また、事故発生に対して適切な対応手順を定めておくこと	対応体制図 手順書（緊急連絡網、フロー図など） 障害対応手順書
6 事業継続計画	時刻認証業務を提供する事業者は、情報システムの重大な故障、自然災害、またはセキュリティ事故等の発生がタイムスタンプ利用者に大きな影響を与える可能性があることを認識して、最悪な事態を避けるためにも、タイムスタンプ利用者への影響を最小限に抑えた事業継続計画を策定し、事業継続に留意すること	事業継続に係る計画書または手順書
4 機密保持	セキュリティ維持にかかわる機密情報の保護、サービス利用者個人情報の保護について適切な措置を講じること	
1 セキュリティ維持にかかわる機密情報の保持	運用者の特定、運用体制、マシン室のレイアウト、監査情報、設備・システムセキュリティ等の機密情報については、その影響度を十分考慮した取扱い方法を定め、それに従った運用を行うこと	機密情報管理規定
2 利用者関連情報保護	利用者にかかわる情報が目的外に利用されたり、不正に漏洩されたりすることがないように、機密範囲とその取扱い方法を定め、それに従った運用を行うこと	個人情報管理規定
3 設備の物理的な隔離	利用者情報や監査情報、設備・システムセキュリティ等の機密情報を保護する保管設備については、施錠を行い物理的に隔離されていること	入退出管理手順 保管場所
5 業務の一時停止・終了	業務一時停止・終了時の利用者への事前通知等の手順が明確に定められていること	
1 事前通知	サービスの一時停止・終了時は、事前にそのスケジュールと手続きを決め、その内容を事前に公知、もしくは利用者へ通知すること	運用規程 サービス約款
2 サービス終了時の移行期間の確保	サービスを終了する際は、利用者が新たな時刻認証業務へ移行するために十分な移行期間を確保すること	運用規程 サービス約款
3 予告なしの業務停止の禁止	障害発生時などの予期できない場合の緊急停止措置以外は、事前の通知なしに業務を一時停止しないこと	運用規程

4 サービス終了時の業務移行措置	前項までを内容に含むサービス終了手続および当該方式においてはTSAによる照合業務終了後はタイムスタンプトークンの有効性が確認できないことについてあらかじめ宣言し、公表しておくこと ただし、技術基準第19項の要件を満たしたタイムスタンプトークン照合用ツールを利用者に提供する場合（ISO/IEC 18014-3［2nd edition 2009-12-15］で規定されている「Extended operation」に対応している場合を除く。）、TSAによる照合業務終了後も当該ツールが動作する期限内においてタイムスタンプトークンの有効性が確認できることをあらかじめ宣言し公表すること	運用規程 サービス約款
6 業務監査	時刻認証業務の適切な運用をチェックするため、定期的に部署外からの適切な業務監査を受け、その結果を認定機関へ開示すること	
1 監査内容	時刻認証業務が本審査基準に沿って適切に実施されていることを確認する業務監査を計画し、実施すること	監査実施要綱 監査計画書
2 監査情報の保管	保管すべき監査情報と保管期間を定めること 保管に当たってはアクセス権限を明確にし、不正アクセスによる情報の改ざん、消去、漏洩等の防止策を講じること	監査実施要綱 監査実施要綱 監査情報保管環境の説明資料
3 監査の頻度	監査の頻度は、最低年１回実施すること	監査実施要綱、監査結果報告書（初回はなし）
4 監査結果の認定機関への開示と対処情報	監査実施後は、認定機関に対して監査結果を速やかに開示するものとし、監査の結果として欠陥が指摘された場合には、以下要件を速やかに対処すること １．欠陥が修正されるまでの対処 （例えば、運用の停止、利用者に対する十分なアナウンス等） ２．指摘された欠陥への対処	監査実施要綱 監査結果報告書（初回はなし） 監査指摘事項への対処計画または結果
7 時刻認証業務の運用に関する記録の取得と保管	時刻認証業務の運用に関する重要な事象およびデータを記録すること、また、記録は全て期間を決めて保管すること	
1 記録する情報の明文化と保管期間	記録する情報対象はその保管期間とともに、文書化しておくこと	運用規程
2 記録する情報の安全な保管と可用性確保	記録する情報は、完全性と機密性を保つとともに必要に応じて利用できるように保管すること	運用規程
3 記録する情報	記録する情報は、本審査基準で保管が求められているものに加えて下記を含むこと a) 時刻配信局より受けた時刻監査記録(または時刻監査証明書のコピー) b) 時刻認証業務にかかわるシステムの動作異常の記録	運用規程
8 システムのトラブル、破壊からの復旧	システムトラブルやシステムの破壊等に対して、緊急停止手段やバックアップデータによる復旧手段を用意すること	
1 時計システムのトラブル対処	タイムスタンプサーバの時計の時刻精度が運用規程の規定範囲外になった場合は、システムトラブルとみなし、システムの緊急停止および復旧作業を速やかに行うこと	障害対応手順書
2 ハードウェア、ソフトウェアまたはデータが破壊された場合の対処	バックアップ用のハードウェア、ソフトウェアまたはデータにより速やかに復旧作業を行うこと	障害対応手順書
9 タイムスタンプトークン生成を行うプログラムの変更および操作	当該プログラムの変更、操作をするときは、以下の要件を満たすこと	
1 当該プログラムの変更	当該プログラムへ変更を加える場合には、変更内容について認定機関に提示し、チェックを受けること	運用手順書

2 当該プログラムの操作	当該プログラムの設定に関する操作は複数人管理で行うこと	運用手順書
3 タイムスタンプトークン生成を行うプロセスの確認	タイムスタンプトークンの生成に係る正常なプロセスの停止もしくは時刻認証業務に不要なプロセスの動作を検知した場合は、権限のあるものへ通知を行い、サービスの停止を行うこと	運用手順書
10 タイムスタンプトークン生成を行うプログラムの改ざん防止	当該プログラムの改ざんを検知した場合は、権限のあるものへ通知を行い、サービスの停止を行うこと	運用手順書
11 照合用データの保管を行うプログラム等の変更および操作	当該プログラム等の変更、操作をするときは、以下の要件を満たすこと	
1 当該プログラムの変更	当該プログラムへ変更を加える場合には、変更内容について認定機関に提示し、チェックを受けること	運用手順書
2 当該プログラムの操作	当該プログラムの設定に関する操作は複数人管理で行うこと	運用手順書
3 プロセス異常時の対応	照合用データの保管に係る正常なプロセスの停止もしくは時刻認証業務に不要なプロセスの動作を検知した場合は、権限のあるものへ通知を行い、サービスの停止を行うこと	運用手順書
12 照合用データの保管を行うプログラムの改ざん防止	当該プログラムの改ざんを検知した場合は、権限のあるものへ通知を行い、サービスの停止を行うこと	運用手順書
13 照合用データのバックアップ		
1 定期的バックアップ	照合用データは定期的にバックアップを行うこと	運用手順書
2 バックアップ作業の管理	照合用データのバックアップおよびリストアは複数人管理で行うこと	運用手順書
14 タイムスタンプトークン照合用データの管理	TSAは、タイムスタンプトークン照合用データを安全に管理すること	
1 タイムスタンプトークン照合用データの保持	TSAは、タイムスタンプトークン照合用データを保持し、その完全性を維持すること	運用手順書
2 タイムスタンプトークン照合用データの確認	TSAは、タイムスタンプトークン照合用データの完全性を定期的に確認すること	運用手順書
3 タイムスタンプトークン照合用データへのアクセス	TSAは、タイムスタンプトークン照合用データのリストア等の変更を加える操作ならびにタイムスタンプトークン照合用データへのタイムスタンプトークン生成システム等からのアクセスに係る設定に変更を加える操作に関して、複数人管理のもとでのみ実行可能とする措置を講じること	運用手順書
4 タイムスタンプトークン照合用データの監査	TSAは、タイムスタンプトークン照合用データの完全性について、定期的に部署外からの監査を受けること	監査実施要綱
5 タイムスタンプトークン照合用データ毀損・滅失時の対応	タイムスタンプトークン照合用データに毀損もしくは滅失が生じた場合の対応手順をあらかじめ策定し、明示しておくこと	運用規程 サービス約款
	タイムスタンプトークン照合用データに毀損もしくは滅失が生じた場合、照合データに係る不具合の発生とその影響（タイムスタンプトークンの失効状況など）を速やかにサービス利用者に通知、もしくは情報公開すること	障害対応手順書

15　リンク情報の生成および照合用データの完全性の確認を行うために用いるプログラム等の管理	リンク情報の生成および照合用データの完全性の確認を行うために用いるプログラム等を安全に管理すること	
1 当該プログラムの変更	当該プログラムへ変更を加える場合には、変更内容について認定機関に提示し、チェックを受けること	運用手順書
2 当該プログラムの操作	当該プログラムの設定に関する操作は複数人管理で行うこと	運用手順書
3 タイムスタンプトークンの照合を行うプロセスの確認	当該プログラムの実行に係る正常なプロセスの停止もしくは時刻認証業務に不要なプロセスの動作を検知した場合は、権限のあるものへ通知を行い、サービスの停止を行うこと	運用手順書
4 技術の危殆化時の対応	リンク情報の生成および照合用データの完全性の確認を行うための技術が危殆化した場合の対応手順をあらかじめ策定し、明示しておくこと	運用規程 サービス約款
	リンク情報の生成および照合用データの完全性の確認を行うための技術が危殆化した場合、照合データに係る不具合の発生とその影響を速やかにサービス利用者に通知、もしくは情報公開すること	障害対応手順書
16　リンク情報の代表値の明証化	TSAは照合用データの完全性を担保するため、あらかじめ定められた規則に従ってリンク情報の代表値を明証化し、かつ明証化の規則を合理的に説明できること	運用手順書 新聞などの掲載情報
17　タイムスタンプトークンの照合を行うプログラムの変更および操作	当該プログラムの変更、操作をするときは、以下の要件を満たすこと	
1 当該プログラムの変更	当該プログラムへ変更を加える場合には、変更内容について認定機関に提示し、チェックを受けること	運用手順書
2 当該プログラムの操作	当該プログラムの設定に関する操作は複数人管理で行うこと	運用手順書
3 プロセス異常時の対応	タイムスタンプトークンの照合に係る正常なプロセスの停止もしくは時刻認証業務に不要なプロセスの動作を検知した場合は、権限のあるものへ通知を行い、サービスの停止を行うこと	運用手順書
18　通信に用いる暗号鍵の管理	TAAとの通信路の安全性を公開鍵暗号技術または共通鍵暗号技術により実現する場合、それらの暗号鍵を安全に管理すること	
1 鍵の生成	鍵の生成は、信頼できる鍵生成システムを利用し、複数人管理のもとで行うこと	運用規程 業務手順書
2 鍵の保管	通信に用いる秘密鍵または共通鍵は、十分なセキュリティが確保できる環境で保管すること	運用規程 業務手順書
3 有効期間	通信に用いる暗号鍵は、用いる暗号技術の最新の安全性評価を元に、適切な有効期間を設けること	運用規程 業務手順書
4 鍵の廃棄	有効期間が経過した鍵や、失効した鍵、危殆化した鍵などは、その後の不正利用が行われないように廃棄すること	運用規程 業務手順書
19　タイムスタンプトークンの有効期限	タイムスタンプトークンの有効期限を適切に定め、利用者に通知すること	
1 タイムスタンプトークンの有効期限の設定と通知	ハッシュアルゴリズムが危殆化すると予測される以前に終了するよう、最新の安全性評価情報を元に、タイムスタンプトークンの有効期限を設定する方法について明確にし、設定の方法と有効期限をユーザに通知すること	運用規程 技術仕様書

2 有効期限の設定、変更の可能性の通知	タイムスタンプトークンの有効期限に関する情報を利用者に通知する際には、時刻認証業務に用いるハッシュ関数の安全性評価や危殆化等によってタイムスタンプトークンの有効期限が設定され、または設定した有効期限が変更される可能性があることを明確に伝えること	運用規程 タイムスタンプトークン

（3）ファシリティの基準

項目	基準（遵守事項）	エビデンス例
1 耐震基準		
1 建築物の耐震性	時刻認証業務用設備を含む建築物は「地震に対する安全性に係る建築基準法」またはこれに基づく命令、条例の規定に適合するものであること	確認通知書、検査通知書、地盤調査書
2 設備の耐震性	時刻認証業務用設備は通常想定される規模の地震による転倒や構成部品の脱落などを防止するための構成部品の固定その他の耐震措置が講じられていること	レイアウト図
2 耐火基準	時刻認証業務に係る設備を含む建築物は建築基準法に規定する耐火建築物または準耐火建築物であること	確認通知書、検査通知書
3 水害防止	水害の防止のための措置が講じられていること	システムの物理的配置を説明する書類
4 電気設備	ビルの電源検査時に無停電で行えること、緊急災害時に業務の継続を確保できるレベルの無停電電源装置、バックアップ発電機などの瞬停対策があること	機器説明書などの確認資料 災害時運用手順書 レイアウト図面
5 火災報知システム	自動火災報知機および消火装置が設置されていること	消防用設備等検査済証等
6 空調設備	時刻認証業務を行うための性能を維持できる温湿度管理されていること	温湿度管理ポリシー
7 認定対象設備に対するアクセス		
1 認定対象設備	時刻認証業務に係るシステム全体を権限ある者のみが開錠可能な別室または錠付きラックにて囲い安全性を確保すること	レイアウト図面 入退室管理の手順書
2 入退室管理	時刻認証業務に係るシステム全体のある部屋およびオペレーションルームの入退室の管理を実施すること 例 バイオメトリックスシステム、ICカードシステムなど	入退室管理手順書

（4）システム安全性の基準

項目	基準（遵守事項）	エビデンス例
1 外部ネットワークとの接続	外部ネットワークからの不正アクセス、攻撃等に対し、それを検知および防御するためのシステム（ファイアウォール等）を備え、必要に応じてセキュリティ更新がなされること	システム構成図（現地確認） セキュリティに関する更新履歴
2 内部ネットワーク（ＬＡＮ）	サービスもしくは機能ごとに、サーバ等機器を適切に配置し、不要な通信を遮断できるようにすること（例：レイヤー3スイッチによる分離） ネットワーク機器は必要に応じてセキュリティ更新がなされること	システム構成図（現地確認） ポートの設定情報 セキュリティに関する更新履歴
3 サーバ・ストレージ		
1 サーバ機能の設定	時刻認証業務にかかる全てのサーバ機能の設定は適切に行うこと（例：不要アクセスの拒否、不要アプリケーション削除、不要ポートの利用停止など）	機能設定確認書
2 セキュリティの運用管理	業務に係る全てのサーバについて適切な運用管理を行うこと（例：十分なテストをした上でのセキュリティパッチ対応、ファイルの整合性の確認、システムログの記録など）	運用手順書

4　システムの可用性	時刻認証業務に係るシステムの障害に備えて、サービスを継続するための対策を実施していること	システム構成図
5　システムの時刻	ログを残す全てのサーバは十分な精度で時刻同期が取れていること	システム運用手順書 時刻同期方法の説明資料

（5）情報開示の基準

項目	基準（遵守事項）	エビデンス例
1　TSAポリシーの公開	以下の内容を含む運用規程を定め、随時参照可能にしておくこと	
1 事業者情報	事業者名、住所、問い合わせ窓口情報（電話、e-mailアドレス等）を明記	運用規程
2 保持している時刻源（時計）とUTCとの最大時刻差	時刻認証業務で使用する時刻ソースの特定情報（OID等）を明記 運用上の確保可能な最大時刻差情報を明記	運用規程
3 時刻監査情報	時刻監査証、監査記録の開示方法を明記（タイムスタンプトークンに時刻監査証または監査記録を含まない場合）	運用規程
4 TAAとのポリシーリンク	時刻認証業務で時刻監査を受けるTAAとのポリシーリンクをOID、URL等により明記	運用規程
5 サービス内容と事業者の義務	時刻認証業務の提供において事業者が提供するサービス内容と事業者が負う義務を明記	運用規程
6 事業者の責任範囲	時刻認証業務の提供に関して事業者が負う賠償責任の範囲と免責事項を明記	運用規程
7 技術情報	時刻認証業務の安全性や信頼性を判断できる技術情報を明記	運用規程
8 タイムスタンプトークンのデータ形式	タイムスタンプトークンのデータ形式を明記	運用規程
9 タイムスタンプトークンに含まれる時刻情報の時系	タイムスタンプトークンに含まれる時刻情報の時系を明記	運用規程
10 暗号アルゴリズムに関する情報	時刻認証業務で使用する暗号アルゴリズムに関して、下記の情報を明記 ・対象となる電子文書のハッシュ値を得るためのハッシュ関数 ・リンク情報の生成に用いるハッシュ関数 ・暗号アルゴリズムが危殆化した場合の対応策 ・暗号アルゴリズムの危殆化が予測される場合の対応策	運用規程
11 リンク情報代表値の明証化方法	リンク情報代表値の明証化方法、明証化時期を明記	運用規程
12 タイムスタンプトークンの有効期限	タイムスタンプトークンの有効期限を設定する方法および設定された有効期限を明記 時刻認証業務に用いるハッシュ関数の安全性評価や危殆化等によってタイムスタンプトークンの有効期限が設定され、または設定した有効期限が変更される可能性があることを明記	運用規程
13 照合のための情報	タイムスタンプトークンの照合に必要な情報を明記 ・照合要求データのフォーマット ・照合要求先の情報	運用規程
14 運用規定	事業者が規定する運用規定を明記	運用規程
15 サービス時間帯	サービスを提供する時間帯を明記	運用規程

16 サービス利用規約	事業者が定めるサービス利用規約を明記 サービス利用に関わる注意事項があれば明記	運用規程
17 利用者個人情報、機密情報に関する取り扱い	情報の取得、管理、保存期間、廃棄、開示に関わる要件を明記	運用規程
18 サービス一時停止・終了時の対応	サービス一時停止・終了時に事業者がとる対応と利用者への通知について明記	運用規程
19 照合データ・リンク情報不整合時の対応	照合データおよびリンク情報に不整合が生じた時に事業者がとる対応と利用者への通知について明記	運用規程
20 システムトラブル等の発生時の対応	システムトラブル、システム破壊、災害発生時に事業者がとる対応と利用者への通知について明記	運用規程
21 準拠法	日本国内法および規制に基づき解釈されることを明記	運用規程
2 利用者および利用者に関わる関係者への情報開示	利用者および利用者に関わる関係者に対して、運用規程の情報公開に加えて、必要に応じて以下の情報を開示すること	
1 問い合わせ情報	利用者用の問い合わせ窓口情報（電話、e-mailアドレス等）	利用者、検証者向け説明資料
2 時刻監査情報	時刻監査証、監査記録	タイムスタンプトークン リポジトリ
3 リンク情報代表値の明証化方法	リンク情報代表値の明証化方法、明証化時期を明記	タイムスタンプトークン リポジトリ
4 タイムスタンプトークンの失効に関する情報	照合データ、リンク情報の不整合等により失効したタイムスタンプトークンの情報を明記	リポジトリ
5 照合のための情報	タイムスタンプトークンの照合に必要な情報を明記 ・照合要求データのフォーマット ・照合要求先の情報	タイムスタンプトークン リポジトリ
6 時刻認証サービス利用に関わる注意事項	運用規程記載以外の注意事項があれば明記 ・タイムスタンプトークンの有効期限とタイムスタンプ付与対象文書の保存期間との関係について明確に注意喚起すること ・タイムスタンプトークン生成に用いるハッシュ関数および有効期限の設定と、電子政府推奨暗号リストとの関係について明記 ・本認定は、有効期限を過ぎたタイムスタンプトークンの信頼・安心を裏付けるものではないことを明記 ・タイムスタンプトークン生成に用いるハッシュ関数の安全性評価や危殆化等によってタイムスタンプトークンの有効期限が設定され、または設定した有効期限が変更される可能性があることを明記 ・タイムスタンプトークン生成に用いるハッシュ関数の危殆化が生じた場合に時刻認証事業者が取る対策（当該ハッシュ関数を用いたタイムスタンプトークンの発行停止、利用者への周知、新サービスへの移行など）を明記	利用者、検証者向け説明資料
7 利用者個人情報、機密情報等に関しての取扱い	利用者個人情報の開示請求手続き等の情報	利用者、検証者向け説明資料 事業者のWebサイト
8 経営情報	利用者が事業者の安定性を判断できる経営情報	公開されているIR情報
3 利用者への通知・連絡	以下の場合には、速やかに利用者へ通知・連絡を行うこと	
1 サービス一時停止・終了時の通知	サービス一時停止・終了時には事前に利用者へ通知すること	通知文書など

2 照合データ、リンク情報不整合時の通知	照合データ、リンク情報に不整合が生じた場合、不整合の発生と影響について速やかに利用者に通知すること	通知文書など
3 システムトラブル等の発生時の通知	システムトラブル、システム破壊、災害発生時には障害の発生と復旧見通しについて速やかに利用者に通知すること	通知文書など
4 開示情報の変更連絡	運用規程や利用者に開示する情報の内容に変更があった場合には、速やかに利用者へ通知すること	連絡文書など